Office de la propriété intellectuelle du Canada

Un organisme d'Industrie Canada

Canadian Intellectual Property Office

An Agency of Industry Canada

Bureau canadien des brevets

Certification

Canadian Patent Office

Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Specification and Drawings, as originally filed, with Application for Patent Serial No: **2,259,089,** on January 15, 1999, by **CERTICOM CORP.,** assignee of Robert J. Lambert, for "Method and Apparatus For Masking Cryptographic Operations".

Sylvie Grégoire

Agent certificateur/Certifying Officer

October 28, 2005

Date

ABSTRACT

A method of masking a cryptographic operation using a secret value, comprising the steps of dividing the secret value into a plurality of parts; combining with each pärt a random value to derive a new part such that the new parts when combined are equivalent to thc original secret value; and utilizing each of the individual parts in the operation.

METHOD AND APPARATUS FOR MASKING CRYPTOGRAPHIC OPERATIONS

This invention relates to cryptographic systems and in particular to a method and apparatus for minimizing successful power analysis attacks on processors.

BACKGROUND OF THE INVENTION

Cryptographic systems generally owe their security to the fact that a particular piece of information is kept secret, without which it is almost impossible to break the scheme. This secret information must generally be stored within a secure boundary, making it difficult for an attacker to get at it directly however, various schemes or attacks have been attempted in order to obtain the secret information. Of particular risk are portable cryptographic tokens, including smart cards and the like. Of the more recent attacks performed on these particularly vulnerable devices are simple power analysis, differential power analysis, higher order differential power analysis and other related techniques. These technically sophisticated and extremely powerful analysis tools can be used by an attacker to extract secret keys from cryptographic devices. It has been shown that these attacks can be mounted quickly and can be implemented using readily available hardware. The amount of time required for these attacks depends on the type of attack and varies somewhat by device. For example it has been shown that a simple power attack (SPA) typically take a few seconds per card, while the differential power attacks (DPA) can take several hours.

Cryptographic operations are performed in a processor operating in a sequential manner by performing a sequence of fundamental operations, each of which generates a distinct timing pattern. Laborious but careful analysis of end-to-end power waveforms can decompose the order of these fundamental operations performed on each bit of a secret key and thus be, analyzed to find the entire secret key, compromising the system.

In the simple power analysis (SPA) attacks on smart cards and other secure tokens, an attacker directly measures the token's power consumption changes over time. The amount of power consumed varies depending on the executed microprocessor instructions. A large calculation such as elliptic curve (EC) additions in a loop and DES rounds, etc, may be identified, since the operations performed with a microprocessor vary significantly during

different parts of these operations. By sampling the current and voltage at a higher rate, i.e., higher resolution, individual instructions can be differentiated.

The differential power analysis attack (DPA) is a more powerful attack than the SPA and is much more difficult to prevent. Primarily, the DPA uses statistical analysis and error correction techniques to extract information which may be correlated to secret keys, while the SPA attacks use primarily visual inspection to identify relevant power fluctuations. The DPA attack is performed in two steps. The first step is recording data that reflects the change in power consumed by the card during execution of cryptographic routines. In the second step, the collected data is statistically analyzed to extract information correlated to secret keys. A detailed analysis of these attacks is described in the paper entitled "Introduction to Differential Power Analysis and Related Attacks" by Paul Kocher et al.

Various techniques for addressing these power attacks have been attempted to date. These include hardware solutions such as providing well-filtered power supplies and physical shielding of processor elements. However, in the case of smart cards and other secure tokens, this is unfeasible. The DPA vulnerabilities result from transistor and circuit electrical behaviors that propagate to expose logic gates, microprocessor operation and ultimately the software implementations.

Accordingly, there is a need for a system for reducing the risk of a successful power analysis attacks and which is particularly applicable to current hardware environments.

SUMMARY OF THE INVENTION

It is an object of this invention to provide a method for minimizing power analysis attacks on processors.

In accordance with this invention there is provided a method of masking a cryptographic operation using a secret value, comprising the steps of:

(a) dividing said secret value into a plurality of parts;

(b) combining with each part a random value to derive a new part such that the new parts when combined are equivalent to the original secret value; and

(c) utilizing each of the individual parts in said operation.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

Figure 1 is a schematic diagram of a communication system; and

Figure 2 is a flow diagram illustrating an embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to figure 1, a communication system having at least a pair of corespondents is shown generally by numeral 10. It is assumed that the correspondents 12 and 14 incorporate cryptographic units 16 and 18 respectively. For convenience, the first correspondent will be referred to as the sender and the second correspondent will be referred to as the receiver. Generally, a plain text message is processed by the encryption unit of the sender and transmitted as cyphertext along a communication channel to the receiver where the encryption message is decrypted by the cryptographic unit 18 to recover the original message. The above system provides a typical environment for application of the invention as will be described below.

Referring to figure 2 a method for masking a private key or secret value used in a cryptographic operation is shown generally by numeral 200. The method comprises the steps of dividing a secret value into a plurality of parts and combining with each part a random value modulo n (where n is the number of points on the elliptic curve) to derive a new part such that the new parts are combined to be equivalent to the original secret value and utilizing each of the individual parts in the operation. Typically, the secret value is a private key, which is used to compute a public key, and more frequently used in signatures, decryption and possibly key exchange protocols, such as Diffie-Hellman key exchange.

For illustrative purposes, we will in the following discussion assume an EC scheme, where P is a point on the elliptic curve. The secret key d is normally combined with the point P to derive dP, the public key. However, the private key may also be used more frequently in various other cryptographic operations as described above. The cryptographic processor is

generally initialized at manufacture time with the public key or secret value d. Initially, the value d may be divided into a number of parts, e.g. $d = b_{10} + b_{20}$.

In a first step the bi's are initialized to $b_1 = b_{10}$ and $b_2=b_{20}$ such that $d = b_{10} + b_{20}$. These initial values of b_1 and b_2 are stored instead of d. Alternatively the d value may also be stored if so desired, however in the case of a smart card where memory is limited this may not be desirable.

Typically when a computation using the value d is required. At a next step, a random number π is generated and the values b1 and b2 are updated as follows:

$$b_1 = b_1 + \pi \bmod n$$

$$b_2 = b_2 - \pi \bmod n$$

The updated values of b_1 and b_2 are stored. Computation is then performed on the point P using the components b_1 and b_2 as follows:

$$dP \bmod n = b_1P + b_2P \bmod n$$

where, P is a point on the curve which is a predefined parameter of the system.

Thus assuming the value π is randomly generated for each session, then an attacker is unlikely to observe a predictable power signature.

In a typical application of the present invention a signature component s has the form:-

$$s = ae + k \pmod n$$

where:

k is a random integer selected as a short term *private* or session key;

$R = kP$ is the corresponding short term *public* key;

$r=R_x$ x component of R

a is the long term private key of the sender;

$Q = aP$ is the senders corresponding public key;

e is a secure hash, such as the SHA-1 hash function, of a message *m* and the short term public key R(or possibly a short message itself); and

n is the order of the curve.

The sender sends to the recipient a message including m, s, and r and the signature is verified by computing the value $R' = (sP\text{-}eQ)$ which should correspond to R. If the computed

values correspond then the signature is verified. Both the secret keys in the above example may be masked using the method of the present invention.

Specifically referring back to the above example, calculation of the product ae may reveal some information on some platforms in some environments. To minimise this, the present invention is applied. The product ae is computed as $ae = (b_0 + b_1)e$ for $(b_0 + b_1) = a$; where b_0, b_1 sum to a. The components b_0 , b_1 are updated periodically as described above. This updating of the components can be made on every new signature operation.

In the above embodiments the secret value was divided into two components b_0 , b_1, however this may be generalized to a plurality of components $b_0 \ldots b_{n-1}$. Furthermore the above signature scheme is used for illustrative purposes and other schemes and operations may equally well be applied using the present invention.

Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of masking a cryptographic operation using a secret value, comprising the steps of:
   (d) dividing said secret value into a plurality of parts;
   (e) combining with each part a random value to derive a new part such that the new parts when combined are equivalent to the original secret value; and
   (f) utilizing each of the individual parts in said operation.

2. A method as defined in claim 1, including generating a plurality of random values.

3. A method as defined in claim 1, said operation being performed in an additive group.

4. A method as defined in claim 1, said operation being performed in a muliplicative group.

5. An article of manufacture comprising:
   (a) a computer usable medium having computer readable program code embodied therein for masking a cryptographic operation using a secret value, the computer readable program code in said article of manufacture comprising;
   (b) computer readable program code configured to cause a computer to divide said secret value into a plurality of parts;
   (c) computer readable program code configured to cause a computer to combine with each part a random value to derive a new part such that the new parts when combined are equivalent to the original secret value; and
   (d) computer readable program code configured to cause a computer to utilize each of the individual parts in said operation.

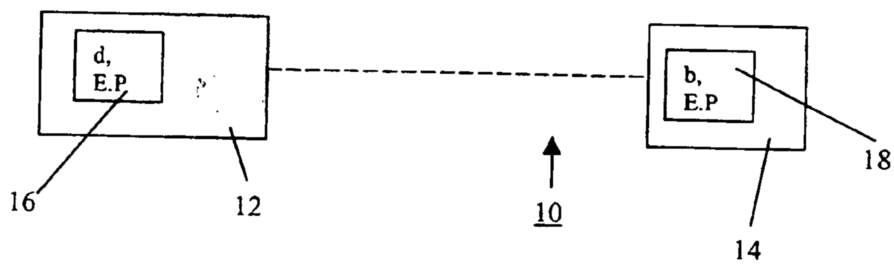
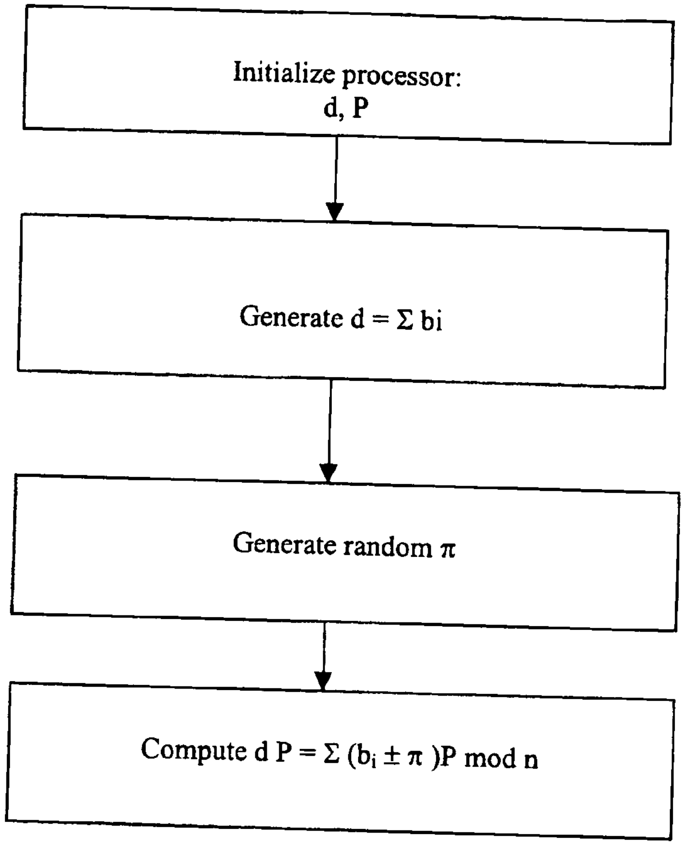


Figure 1


Initialize processor:
d, P
Generate $d = \Sigma$ bi
Generate random π
Compute $d P = \Sigma (b_i \pm \pi) P \bmod n$

200

Figure 2